

NASA Information Technology Requirement

NITR 2810-24

Effective Date: January 28, 2010

Expiration Date: May 16, 2011

NASA IT Device Vulnerability Management

Responsible Office: Office of the Chief Information Officer

Table of Contents

Change History

PREFACE

P.1 PURPOSE

P.2 APPLICABILITY

P.3 AUTHORITY

P.4 APPLICABLE DOCUMENTS

P.5 CANCELLATION

REQUIREMENTS AND RESPONSIBILITIES

Appendix A: Definitions

Appendix B: Glossary

Distribution

NODIS

Change History

NITR 2810-24, NASA IT Device Vulnerability Management

Change Number	Date	Change Description
1		
2		
3		
4		
5		

PREFACE

P.1 PURPOSE

a. The National Aeronautics and Space Administration (NASA) faces ever increasing IT security challenges in balancing its Space Act mandate, its reliance on information technology and the Internet, and a distributed enterprise network architecture. One way that NASA meets this challenge is by employing a layered approach to IT security. NASA has deployed security measures at the enterprise network level, the local network level, the IT system level, and at the individual device level.

b. There are more than 120,000 devices or nodes located at NASA Centers and Facilities, and connected to NASA networks. Each of these nodes can be a potential vector for unauthorized access, virus infection, or some other security incident. The purpose of this policy is to protect each device by defining standard security measures against viruses and other malware, ensuring patches are applied, setting requirements for vulnerability scans, and establishing an inventory of all devices and their security configurations.

P.2 APPLICABILITY

This document applies to all NASA Centers, facilities, employees, contractors (as provided by law or contract), recipients of NASA grants and cooperative agreements, partners and visitors, where appropriate, in achieving NASA missions, programs, projects, and institutional requirements.

With the exception of classified systems, the requirements in this document apply to all IT devices connected to NASA networks and to all NASA IT devices regardless of what networks (mission, non-mission, lab, isolated, etc.) such devices are connected to. This document does not apply to non-NASA devices connected to NASA guest networks.

P.3 AUTHORITY

Reference paragraph P.3, NPR 2810.1A, Security of Information Technology.

P.4 APPLICABLE DOCUMENTS

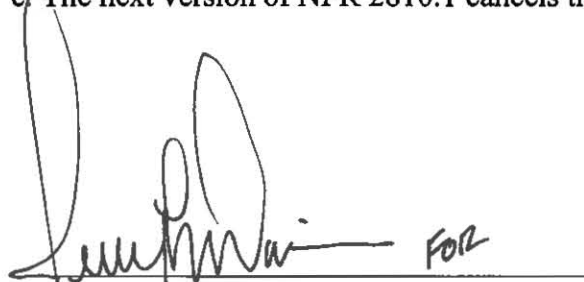
- a. NASA NPR 2810.1A. Security of Information Technology.
- b. NITR-2800-1 NASA IT Waiver Process
- c. NASA-STD-2804 Minimum Interoperability Software Suite

P.5 MEASUREMENT AND VERIFICATION

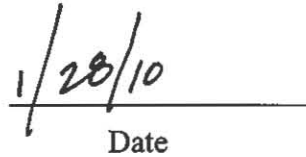
The NASA Chief Information Security Officer (CISO) shall provide annual assessment of the Agency common and hybrid security controls SI-1, SI-4, and RA-1.

P.6 CANCELLATION

- a. ITS-SOP-0012 Patch Selection and Reporting Requirements.
- b. Memorandum 04-04-2007 – FY 2007 and FY 2008 Patch Management and Security Configuration Metrics.
- c. The next version of NPR 2810.1 cancels this NITR.

A handwritten signature in black ink, appearing to read 'Linda Y. Cureton', is written over a horizontal line. To the right of the signature, the word 'FOR' is handwritten in a similar style.

Linda Y. Cureton
Chief Information Officer

A handwritten date '1/28/10' is written in black ink over a horizontal line. Below the line, the word 'Date' is printed in a standard font.

1.0 Device Inventory

1.1 Requirements.

1.1.1 All NASA IT devices shall be associated with a registered NASA System Security Plan (SSP).

1.1.2 The Certification and Accreditation packages of all NASA information systems shall have an asset inventory listing all IT devices associated with the information system.

1.1.3 IT Security Enterprise Data Warehouse (ITSEC-EDW) shall be the Agency consolidated IT security inventory of IT devices.

a. All NASA IT devices and all devices on NASA non-guest networks shall be recorded and tracked within the ITSEC-EDW.

b. All NASA IT devices recorded in the inventory shall be associated, in ITSEC-EDW, with an SSP.

c. ITSEC-EDW shall collect and correlate patch statistics, vulnerability scan results, hardware and software data, security configurations, and information from other data sources.

d. NASA IT devices shall be automatically detected on NASA networks and recorded in ITSEC-EDW (via patch reporting updates, network vulnerability scans, etc.) or manually registered in ITSEC-EDW.

1.2 Roles and Responsibilities.

1.2.1 Information System Owners (ISO) shall:

a. Be responsible for identifying and documenting, in the SSP, the inventory of all devices associated with their information system(s).

b. Ensure that all NASA IT devices, which are part of the information system, are recorded in ITSEC-EDW and are associated with their system's SSP in ITSEC-EDW.

1.2.2 The Agency Security Update Service (ASUS) project shall maintain the ITSEC-EDW in support of IT Device Inventory requirements.

2.0 Malware Protection

2.1 Requirements.

2.1.1 Antivirus software shall be installed, and maintained up to date, on all NASA IT devices that can run antivirus software.

a. Antivirus software shall be appropriate to the system (see NASA-STD-2804).

b. The installed antivirus software shall be currently supported by the publisher or appropriate third-party.

c. Antivirus software shall be updated as needed.

d. Antivirus signatures shall be routinely updated, on a daily basis.

e. Information systems with a FIPS199 security category of Moderate or High shall automatically update the antivirus software and signatures.

f. Information systems with a FIPS199 security category of Moderate or High shall utilize centrally-managed antivirus protection.

g. Information systems with a FIPS199 security category of Moderate or High shall ensure that only privileged users may make changes to the antivirus software configuration, including the ability to skip updates or not scan files automatically.

2.1.2 Any NASA IT device not compliant with these requirements shall be disconnected from the network and only re-connected once the compliance issues have been resolved.

2.2 Roles and Responsibilities.

2.2.1 ISOs shall ensure that for all NASA IT devices that are part of their information system:

- a. Antivirus software is installed and updated as required , and
- b. Antivirus signatures are current.

2.2.2 Information Technology Security Managers (ITSMs) shall:

- a. Provide oversight to ensure antivirus requirements are met.
- b. Coordinate the generation of antivirus status reports.

3.0 Patch Management

3.1 Requirements.

3.1.1 All NASA IT devices shall be patched with all applicable patches and hot-fixes to address functionality, stability, and security issues.

3.1.2 The NASA patch management baseline shall consist of all current vendor critical patches and is the list of patches and fixes that shall be installed on all applicable systems. (NASA considers the highest vendor rating of patches as equal to the “critical” rating because some vendors call their highest patch rating other names (e.g., “high” or “important”).

3.1.2.1. Patches in the NASA patch management baseline shall be applied to all applicable devices within 30 calendar days of the release of the patch. This allows time to appropriately test the patch(es) at each Center and then deploy the patch(es) to applicable devices.

3.1.3 Expedited patches shall be applied to all applicable devices within 7 business days. (The CISO or designee may deem certain patches of an especially urgent nature and may assign these patches the “expedited” designation. Expedited patches are patches that represent a serious threat to the IT security posture of the Agency).

3.1.4 The current patch status of all NASA workstations and servers and of all workstations and servers on NASA networks shall be reported in ITSEC-EDW. (This includes all test and lab devices, and devices connected to isolated networks).

3.1.5 To fulfill patch reporting requirements, all NASA IT devices and all devices on a NASA non-guest network shall either :

- a. Have the Agency patch management/reporting software agent installed. The software agent automatically reports patch status to the ITSEC-EDW. This requirement is applicable to all devices that can execute the Agency patch management/reporting software agent; or

b. Be registered in the ITSEC-EDW, with patch status reported manually in ITSEC EDW by the second Monday of each month. This requirement applies only to devices that cannot execute the Agency patch management/reporting software agent.

3.1.6 All installed patch management/reporting software agents shall be configured to report to the appropriate patch management server.

3.1.6.1. All patch management/reporting software agents shall be grouped by SSP on the relevant patch management server.

3.1.7 All Agency patch management servers shall automatically send updates to the ITSEC-EDW database.

3.1.7.1. The update schedule shall be determined by the ASUS Project Manager.

3.2 Roles and Responsibilities.

3.2.1 The ASUS project provides patch management and patch reporting support and guidance to all NASA organizations. The ASUS project shall:

- a. Coordinate the management of the patch management and reporting solution, including version control, across the Agency.
- b. Provide guidance and assistance to Center patch management server administrators in managing the patch management and reporting solution at the Center.
- c. Generate monthly and expedited patch status and patch compliance reports on NASA IT devices, based on Center-reported data.
- d. Report to the NASA Office of the Chief Information Officer (OCIO) and to the ITSMs, any NASA IT devices recorded in ITSEC-EDW that do not have the patch management/reporting software agent installed and that have not been registered manually.
- e. Report to the NASA OCIO and to the ITSMs, any NASA IT devices recorded in ITSEC-EDW that are not associated with an SSP.

3.2.2 Information System Owners shall:

- a. Ensure that all NASA IT devices are patched and their patch status is reported in accordance with the requirements in section 3.1.
- b. Ensure that the Agency patch management/reporting agent software is installed and running on all of their NASA IT devices that can execute the software.
- c. Ensure that patch management/reporting software agents on devices, which are part of their information system, are grouped by System Security Plan (SSP) within the local patch management server.
- d. Ensure that NASA IT devices that are not running the patch management/reporting software agent are recorded and registered in ITSEC-EDW.

3.2.3 ITSMs shall:

- a. Oversee the patch management and reporting activities at their Center to ensure that the requirements are met.
- b. Ensure that patch management reports are made available to the ISOs at the Center as needed.

- c. Ensure that Center organizations are utilizing the appropriate patch management/reporting solution as defined by the ASUS project.
- e. Ensure communication between Center patch management servers and the ITSEC-EDW.

4.0 Network-based Vulnerability Scanning

4.1 Requirements.

4.1.1 All NASA IT devices and all devices on NASA networks, shall be subjected to routine (at least monthly) network based vulnerability scans using the NASA approved vulnerability scanning tool and the Agency scan profile.

4.1.2 The NASA vulnerability management scan profile shall consist of all current high, non-intrusive, non-credentialed vulnerability signatures. (NASA considers the highest severity rating in the scanning tool as equal to the “high” rating because some vendors call their highest vulnerability severity rating other names).

4.1.2.1. All vulnerabilities in the Agency scan profile shall be mitigated within 30 calendar days of discovery on all affected devices.

4.1.3 Expedited mitigations shall be applied to all affected devices within 7 business days. (The CISO or designee may deem certain vulnerabilities of an especially urgent nature because they represent a serious threat to the IT security posture of the Agency and may assign the mitigation of these vulnerabilities the “expedited” designation.).

4.1.4 Each Center shall run an appropriate version of the Agency approved scanning tool as set by the NASA Vulnerability Scanning and Assessment Team (VSAT) with current vulnerability signature definitions.

4.1.5 All Center vulnerability scanning servers shall automatically send all scan results to the ITSEC-EDW database.

4.1.5.1 The update schedule shall be coordinated and disseminated by the VSAT and the ASUS project.

4.1.6 Any NASA devices and any devices found on NASA networks that continue to exhibit the same (unmitigated or un-accepted) vulnerabilities identified in three consecutive monthly scans, shall be disconnected from the network and only re-connected once the vulnerabilities are eliminated or mitigated.

4.1.6.1 Center Chief Information Officers (CIOs), ITSMs, or ISOs may choose to disconnect such a device sooner depending on the severity of the vulnerabilities or sensitivity of the device.

4.2 Roles and Responsibilities.

4.2.1 The VSAT provides support and guidance on network vulnerability scanning to all NASA organizations. The VSAT shall:

- a. Maintain the Agency hardware, software and support licensing for, and provide training on, the Agency approved vulnerability scanning tool.
- b. Manage software versions of the Agency approved vulnerability scanning tool.
- c. Work with Center vulnerability scanning points of contact to ensure that Center vulnerability scan data is reported in accordance with requirements.

d. Create Center and Agency reports based on Center vulnerability scanning data.

4.2.2 Information System Owners shall:

a. Ensure that all NASA IT devices are available for network based vulnerability scanning and reporting in accordance with these requirements.

b. Ensure elimination or mitigation of all known high vulnerabilities, at minimum, and for ensuring that previously identified vulnerabilities continue to be mitigated.

4.2.3 ITSMs shall:

a. Oversee the vulnerability scanning, reporting, and mitigation activities at their Center to ensure that the requirements are met.

b. Ensure that vulnerability scan reports are made available to the ISOs at the Center for remediation.

c. Ensure the Center is utilizing the appropriate scanner version as defined by the VSAT.

d. Ensure the Center maintains current vulnerability definitions and scan signatures.

e. Ensure communication between Center vulnerability scanner databases and the ITSEC-EDW.

5.0 Waivers

5.1 Waivers shall be submitted in accordance with the NASA IT Waiver process and procedures (see NITR-2800-1, NASA IT Waiver Process).

5.2 All approved waivers to the requirements in sections 2.1.1, 2.1.2, 3.1.2.1, 3.1.1, 3.1.3, 3.1.5.a, 4.1.1, 4.1.2.1, and 4.1.3 of this policy shall be documented in the information system's Plan of Actions and Milestones (POA&M), to include corrective actions, mitigating controls, and risk acceptances as needed.

Appendix A Definitions

Agency Security Update System (ASUS) Project	The ASUS project is a part of the NASA Information Technology Security Program, which is under the management of the NASA CIO. ASUS provides NASA organizations with tools, processes, and procedures that facilitate patch management and reporting.
External System	An Information Technology System that handles, processes, or transmits NASA data but is not in NASA IP space.
Information System. (Also referred to as IT System)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.[44 U.S.C., Sec. 3502] (Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.) [NIST]
IT Device	A network endpoint or node regardless of its operating system or type, such as a desktop, laptop, server, printer, including network infrastructure hardware (firewall, router, switch, hub, etc.) capable of storing, processing or transmitting data. This includes external storage such as USB drives, mobile phones, and media players.
IT Security Enterprise Data Warehouse (ITSEC-EDW)	IT Security Enterprise Data Warehouse (ITSEC-EDW) is the Agency solution being developed by OCIO as the inventory of NASA IT devices and their security configurations. It will have consolidated patch statistics, vulnerability scan results, hardware and software data, and correlation capabilities
NASA IT Device	An IT device which is covered or is required to be covered under a NASA system security plan (SSP), whether government issued or provided by an external entity. This excludes those devices that are considered part of an external system
NASA Network	Any IT network funded by NASA or on a NASA facility
Patch	Any vendor/developer issued update to hardware, software or firmware that is intended to address the secure operation (confidentiality, integrity, availability) of a device. Some organizations may refer to these kind of updates as a “hotfix,” a “maintenance release,” a “service pack,” or an “update.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished, resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.[OMB Memorandum 02-01] (NIST)
Vulnerability Scanning and Assessment Team	The VSAT is primarily responsible for the management of the network vulnerability scanning tools (Foundstone) and program. The VSAT will, among other things, make sure that scan signatures are current and that the

	scanners are communicating across the Foundstone architecture, and that communication between the central Foundstone device and ITSEC-EDW is operational.
Scan Profile	Defines the what, when, and how of a vulnerability scan activity. The Agency scan profile will scan for all high vulnerabilities, what ip addresses are covered in the scan. The scan will be performed once a month but the profile will define the time of day (or details, such as, time period in a 24 hour period, etc.). It will define if the scan will include port scanning, credentialed vulnerability scanning, or bandwidth throttling.
Security Configuration	<p>Elements of a software's security that can be altered through the software itself. Examples of settings are an operating system offering access control lists that set the privileges that users have for files, and an application offering a setting to enable or disable the encryption of sensitive data stored by the application. FDCC is an example of a collection of software (in this case the Windows Operating System) elements, the particular settings of which, are configured to enhance the system's security.</p> <p>National Institute of Standards and Technology Interagency Report 7502 (Draft) (June 2009)</p>
Server	A computer that stores application and data files for all workstations on a network; Usually, a server runs a specific server operating system such as Windows Server 2000/2003/2008, or Sun Solaris 9, 10, etc.
System Security Plan (SSP)	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-18]
System	See Information system
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [CNSS Inst. 4009, Adapted]
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system. [CNSS Inst. 4009]
Workstation	A workstation is a high-end microcomputer designed for technical or scientific applications. Intended primarily to be used by one person at a time, they are commonly connected to a local area network. Usually a workstation runs a specific operating system such as Windows XP, Linux, Unix, or some other

Appendix B Acronyms

ASUS	Agency Security Update Service team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ISO	Information System Owner
IT	Information Technology
ITSEC-EDW	IT Security Enterprise Data Warehouse
ITSM	Information Technology Security Manager
NASA	National Aeronautics and Space Administration
NITR	NASA Interim Technical Requirement
OCIO	Office of the Chief Information Officer
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SI	System and Information Integrity
SI	System Information and Integrity (family of security controls)
SOP	Standard Operating Procedure
SSP	System Security Plan
VSAT	Vulnerability Scanning and Assessment Team